IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

LOUJAIN HATHLOUL ALHATHLOUL, Plaintiff, v. **DARKMATTER GROUP**, **MARC BAIER**, **RYAN ADAMS**, and **DANIEL GERICKE**, Defendants.	Case No. 3:21-cv-01787-IM **OPINION AND ORDER GRANTING DEFENDANTS' MOTION TO DISMISS**

Bridget M. Donegan, Boise Matthews, L.L.P., 805 SW Broadway, Suite 1900, Portland, OR 97205. Christopher E. Hart and Anthony D. Mirenda. Foley Hoag, L.L.P., 155 Seaport Boulevard, Boston, MA 02210. David Greene, Mukund Rathi, Electronic Frontier Foundation, 815 Eddy Street, San Francisco, CA 94109. Attorneys for Plaintiff Loujain Hathloul Alhathloul.

Nicholas F. Aldrich, Schwabe, Williamson & Wyatt, P.C., 1211 SW 5th Ave., Suite 1900, Portland, OR 97204. Anthony T. Pierce, Caroline L. Wolverton, Akin Gump Strauss Hauer &

Feld L.L.P., 1333 New Hampshire Avenue, N.W., Washington, DC 22036. Natasha G. Kohne, Akin Gump Strauss Hauer & Feld, L.L.P., 580 California St., Suite 1500, San Francisco, CA 94104. Attorneys for Defendant DarkMatter Group.

Clifford S. Davidson, Snell & Wilmer L.L.P., 1455 SW Broadway, Suite 1750, Portland, OR 97201. Attorney for Defendants Marc Baier, Ryan Adams, and Daniel Gericke.

IMMERGUT, District Judge.

Before this Court is Defendants DarkMatter Group, Marc Baier, Ryan Adams, and Daniel Gericke's (collectively "Defendants") Motion to Dismiss. ECF 28. Defendants argue that this Court lacks personal jurisdiction over Defendants or, in the alternative, that Plaintiff Loujain Hathloul Alhathloul ("Plaintiff") has failed to state a claim upon which relief can be granted.

Plaintiff brings three federal claims against Defendants, based on allegations that Defendants hacked Plaintiff's iPhone, surveilled her movements, and exfiltrated her confidential communications for use against her by the security services of the United Arab Emirates ("UAE"). ECF 1 at ¶¶ 1, 134, 165, 171. According to Plaintiff, Defendants' actions led to her arrest by the UAE security services and rendition to Saudi Arabia, where Plaintiff states that she was detained, imprisoned, and tortured. *Id.* Plaintiff's allegations of political retaliation and torture are highly concerning. Nevertheless, this Court is bound by jurisdictional limits and grants Defendants' Motion to Dismiss for lack of personal jurisdiction.[1]

BACKGROUND

Plaintiff is a Saudi human rights activist and leader of the movement to promote the rights of women and girls in the Kingdom of Saudi Arabia ("Saudi Arabia"). ECF 1 at ¶ 1. Defendant DarkMatter is an Emirati company. *Id.* at ¶ 6. Defendants Marc Baier, Ryan Adams,

[1] Because this Court finds that it cannot exercise personal jurisdiction over any of the named Defendants, it declines to consider whether Plaintiff has adequately stated a claim upon which relief can be granted.

and Daniel Gericke are former senior executives at DarkMatter. *Id.* at ¶ 1. Plaintiff alleges, on information and belief, that Defendant Baier is domiciled in the UAE and that Defendant Gericke is domiciled in Singapore. *Id.* at ¶¶ 7–8. Plaintiff also alleges that Defendant Adams is domiciled in the state of Oregon, *id.* at ¶ 9, an allegation that Defendants contest, ECF 28 at 13.[2]

Plaintiff alleges that beginning in or about 2008, the UAE sought out U.S. corporations to build a cyber-surveillance program known as Project Raven, the purpose of which was to target and hack perceived dissidents from the UAE and Saudi Arabia, including human rights activists. ECF 1 at ¶ 51. In or about 2009, Plaintiff alleges that a Maryland-based company known as CyberPoint International, LLC ("CyberPoint") became the UAE's primary contractor on Project Raven. *Id.* at ¶ 52. Plaintiff alleges that Defendants Baier, Adams, and Gericke all worked for CyberPoint at various periods between 2012 and 2015. *Id.* at ¶¶ 57–59. Plaintiff further alleges that while working at CyberPoint, Defendants Baier, Adams, and Gericke "developed and operated Project Raven to target and hack individuals and organizations designated by the UAE." *Id.* at ¶ 60.

Plaintiff alleges that beginning in or about late 2015 or early 2016, the UAE transitioned cyber services under Project Raven from CyberPoint to Defendant DarkMatter. *Id.* at ¶ 67. Plaintiff further alleges that on or about December 31, 2015, CyberPoint terminated its employment with Defendants Baier, Adams, and Gericke and that Defendants Baier, Adams, and

[2] In their Motion to Dismiss, Defendants state that "Adams is *not* domiciled in Oregon." ECF 28 at 13. Defendants do not state where Adams is domiciled, but argue that "Rule 4(k)(2) does not provide jurisdiction over Adams for the same reasons that it does not provide jurisdiction over Baier and Gericke." *Id.* at 14. For the purposes of this Opinion and Order, and consistent with Plaintiff's jurisdictional argument, this Court will proceed to analyze all Defendants under Rule 4(k)(2). *See* ECF 35 at 12, n.3 ("Accordingly, and similar to the other Individual Defendants, Ryan Adams would be subject to jurisdiction under Rule 4(k)(2) if his contacts satisfy the minimum contacts test with the U.S. as a whole.").

Gericke subsequently became employees of DarkMatter. *Id.* at ¶ 69. Plaintiff alleges that when they joined DarkMatter, Defendants Baier, Adams, and Gericke transferred technology and knowhow developed at CyberPoint to DarkMatter, in violation of U.S. law. ECF 35, Ex. A at ¶¶ 32–33.[3] Plaintiff further alleges that Defendants Baier, Adams, and Gericke recruited U.S. employees to join them at DarkMatter. *Id.* at ¶ 35. In September of 2021, Defendants Baier, Adams, and Gericke entered into a Deferred Prosecution Agreement ("DPA") with the U.S. Department of Justice arising out of their conduct while employees at CyberPoint and DarkMatter. ECF 1 at ¶ 131; *see generally* ECF 35, Ex. A.

Through Defendants Baier, Adams, and Gericke, Plaintiff alleges that Defendant DarkMatter began running "zero-click" exploits, which can install unwanted code on a target's phone without the target's awareness or authorization. *Id.* at ¶¶ 78–80. Plaintiff further alleges that Defendants purchased these "zero-click" exploits from other U.S. companies. ECF 35, Ex. A at ¶¶ 45, 66; ECF 1 at ¶ 84. The technology purchased from other U.S. companies "had features that limited [its] effectiveness as a computer hacking tool." ECF 35, Ex. A at ¶¶ 47, 54. Plaintiff alleges that Defendants later "modified" and "upgraded" this technology to create the specific type of "zero-click" exploit used to hack Plaintiff's phone. ECF 35, Ex. A at ¶¶ 49, 56; ECF 1 at ¶¶ 84, 168. These upgrades included combining the technology with "other malicious software," creating a "graphic operator interface," creating anonymous delivery mechanisms, and creating

[3] Though not attached to Plaintiff's Complaint, Plaintiff submitted the Deferred Prosecution Agreement ("DPA") between the Individual Defendants and the U.S. Department of Justice and asks this Court to take judicial notice of the DPA pursuant to Federal Rule of Evidence 201(b), which allows a court to "judicially notice of a fact that is not subject to reasonable dispute because it. . .can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." ECF 35 at 2 n.1. Defendants do not address Plaintiff's request in their Reply In Support of Defendants' Motion to Dismiss. Accordingly, this Court takes judicial notice of the facts contained in the DPA.

"anonymized . . . pathways to exfiltrate data and information." ECF 35, Ex. A at ¶¶ 56, Once upgraded, these "zero-click" exploits, Plaintiff alleges, allowed Defendant DarkMatter to deploy iMessages—messages sent through the Apple operating system to Apple devices—to install malware on a target's iPhone and obtain, among other things, a target's emails, location data, text messages, and photographs. ECF 1 at ¶¶ 78, 82–83.

Plaintiff alleges, based on information and belief, that the "zero-click" exploit utilized servers located in the United States to reach Plaintiff's device located in the UAE. *Id.* at ¶¶ 87, 108. Plaintiff further alleges that to execute these exploits, Defendants must interact with Apple's servers in the United States in several ways. First, the attacker must obtain the target's encryption and routing information from Apple's servers. *Id.* at ¶ 89. Next, the attacker encrypts the iMessage using the information from the identity servers and sends the iMessage to the Apple Push Notification Service, which temporarily stores and sends data to Apple device users. *Id.* at ¶ 90. Finally, Plaintiff alleges that because malware is a large attachment, the attachment is encrypted and uploaded to Apple's storage servers. *Id.* at ¶ 92. As such, Plaintiff alleges that any exploit sent to a foreign target must interact with Apple's servers, which Plaintiff alleges are based in the United States, "several times." *Id.* at ¶ 93. Notably, Plaintiff alleges that Defendants used a custom program to do this that "sends a specifically crafted iMessage, containing an exploit and malware, to servers located in the United States to reach the target's device." *Id.* at ¶ 88.

Plaintiff alleges that Defendant DarkMatter hacked her iPhone using this "zero-click" exploit, surveilled her movements, and exfiltrated her confidential communications to the UAE's security services. *Id.* at ¶¶ 108–115. Following the hack, Plaintiff alleges that the UAE limited her international travel solely to Saudi Arabia, arbitrarily detained her, and forcibly rendered her

to Saudi Arabia in March of 2018. *Id.* at ¶¶ 114, 117–18. While in the custody of Saudi Arabia, Plaintiff alleges that she was subjected to interrogation and torture. *Id.* at ¶¶ 124–25.

Plaintiff filed the instant case on December 9, 2021. *Id.* at 39. Plaintiff alleges three claims under federal law against all Defendants. First, Plaintiff alleges four separate violations of the Computer Fraud and Abuse Act ("CFAA"). Second, Plaintiff alleges conspiracy to violate the CFAA. Third, Plaintiff alleges persecution as a crime against humanity under the Alien Tort Statute.

LEGAL STANDARD

A. Motion to Dismiss for Lack of Personal Jurisdiction

"Where a defendant moves to dismiss a complaint for lack of personal jurisdiction, the plaintiff bears the burden of demonstrating that jurisdiction is appropriate." *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004) (citation omitted). "Where . . . a defendant's motion to dismiss is based on a written record and no evidentiary hearing is held, 'the plaintiff need only make a prima facie showing of jurisdictional facts.'" *Picot v. Weston*, 780 F.3d 1206, 1211 (9th Cir. 2015) (citation omitted). Uncontroverted allegations in the complaint must be taken as true. *Boschetto v. Hansing*, 539 F.3d 1011, 1015 (9th Cir. 2008). However, a court need not accept as true "threadbare recitals of a cause of action's elements, supported by mere conclusory statements" *Ashcroft v. Iqbal*, 556 U.S. 662, 663 (2009).

Under Federal Rule of Civil Procedure 4(k)(2), "[f]or a claim that arises under federal law," a court may exercise personal jurisdiction over a defendant "not subject to jurisdiction in any state's courts of general jurisdiction" if "exercising jurisdiction is consistent with the United States Constitution and laws." Fed. R. Civ. P. 4(k)(2). Rule 4(k)(2) requires (1) a federal claim, (2) a defendant not subject to personal jurisdiction in any state, and (3) that "the federal court's

exercise of personal jurisdiction . . . comport[s] with due process." *Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 461 (9th Cir. 2007).

A federal court's exercise of personal jurisdiction comports with due process where a defendant has "certain minimum contacts" with the forum state "such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'" *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945). From this general principle, courts have recognized two distinct categories of personal jurisdiction: general, or "all-purpose" jurisdiction, and specific, or "case-linked" jurisdiction. *Ford Motor Co. v. Mont. Eighth Jud. Dist. Ct.*, 141 S. Ct. 1017, 1024 (2021) (citing *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 919 (2011)).

A court can exercise general jurisdiction over a defendant in any forum where the defendant "is 'essentially at home' . . . ." *Id.* (quoting *Goodyear*, 564 U.S. at 919). An individual is subject to general jurisdiction in their place of domicile, while a corporation is subject to general jurisdiction in its place of incorporation and principal place of business. *Id.* (citations omitted). A court can exercise specific jurisdiction over a defendant, by contrast, only where the "defendant's suit-related conduct [] create[s] a substantial connection with the forum State." *Walden v. Fiore*, 571 U.S. 277, 284 (2014).

The Ninth Circuit uses a three-part test to evaluate whether a defendant has sufficient "minimum contacts" with the forum state such that exercise of specific jurisdiction comports with due process:

> (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws; (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and (3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e., it must be reasonable.

CollegeSource, Inc. v. AcademyOne, Inc., 653 F.3d 1066, 1076 (9th Cir. 2011) (quoting

Schwarzenegger, 374 F.3d at 802). The personal jurisdiction analysis under Rule 4(k)(2) is "nearly identical to the traditional personal jurisdiction analysis with one significant difference: rather than considering contacts between [the defendant] and the forum state, [courts] consider contacts with the nation as a whole." *AMA Multimedia, LLC v. Wanat,* 970 F.3d 1201, 1208 (quoting *Holland Am. Line*, 485 F.3d at 462).

The first part of the Ninth Circuit's specific jurisdiction analysis refers to both purposeful direction and purposeful availment. *Mavrix Photo, Inc. v. Brand Techs., Inc*., 647 F.3d 1218, 1228 (9th Cir. 2011). Courts apply the purposeful direction analysis, also known as the "effects test," to conduct that occurs outside of the forum state but whose effects are felt within the forum state. *Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 605 (9th Cir. 2018). For conduct that occurs within the forum state, by contrast, courts within the Ninth Circuit apply the purposeful availment test. *Id.* at 604.

The plaintiff "bears the burden of satisfying the first two prongs." *CollegeSource*, 653 F.3d at 1076. If the plaintiff does so, the burden shifts to the defendant at prong three "to set forth a 'compelling case' that the exercise of jurisdiction would not be reasonable." *Id*. (quoting *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476–78 (1985)).

ANALYSIS

A. This Court Cannot Exercise Personal Jurisdiction over Defendants

Though Plaintiff names Defendant DarkMatter and Defendants Baier, Adams, and Gericke as separate defendants, the conduct underpinning this Court's jurisdictional analysis is the same for all named defendants. As such, this Court will evaluate whether it can exert personal jurisdiction over Defendants collectively.

Defendants argue Plaintiff alleges no jurisdictionally significant connection between Defendants, the present litigation, and the United States, save for the fact that certain text messages allegedly sent by Defendant DarkMatter from a foreign location passed through U.S. servers on their way to Plaintiff's phone abroad. ECF 28 at 1. Plaintiff counters that Defendants contacts with the United States are jurisdictionally significant because Defendants caused Apple's U.S. servers to transmit malicious code to Plaintiff's phone. ECF 35 at 13.

For the following reasons, this Court concludes that it cannot exercise personal jurisdiction over Defendants.

1. Defendants Did Not Purposefully Direct Their Actions at the United States

a. Purposeful Direction, Rather than Purposeful Availment, Guides this Court's Jurisdictional Analysis

As an initial matter, Plaintiff urges this Court to apply the purposeful availment analysis to her jurisdictional claim. ECF 35 at 13. Existing Ninth Circuit precedent, however, dictates that the purposeful direction test, and not the purposeful availment test, applies to tortious conduct that occurs outside of the forum. *Freestream*, 905 F.3d at 605.

Plaintiff argues that the purposeful availment inquiry is appropriate in the present case because part of the allegedly tortious conduct—Defendants' transmission of the message that resulted in the hack of Plaintiff's phone through a server based in the United States—took place in the United States. ECF 35 at 14. To support her argument, Plaintiff points to language from the CFAA which states that it is a crime for anyone to "knowingly cause[] the transmission of a program, information, code, or command" which "intentionally causes damage without authorization, to a protected computer." ECF 35 at 15; 18 U.S.C. § 1030(a)(5)(A). At the outset, this Court notes that torts committed in the virtual realm add a layer of complication to the traditional analysis of whether conduct occurs inside or outside of the forum state. As another

court in this circuit has noted, courts are split as to whether a tortious act committed virtually occurs at the location where the defendant is "physically typing on the keyboard" (or, in this case, physically pressing send on an iMessage) or at the location "that contains the computer hardware manipulated by the defendant to commit the tort." *HB Prods., Inc. v. Faizan*, 603 F. Supp. 3d 910, 922 (D. Haw. 2022). The Ninth Circuit, for its part, has yet to squarely this question.

Under either formulation, however, this Court finds that the allegedly tortious conduct took place outside of the forum. If this Court were to base its determination of where the tortious conduct took place on the location where the Defendants sent the message, that location would be outside of the forum. *See id.* Conversely, if this Court were to base its determination of where the tortious conduct took place on the location "that contain[ed] the hardware manipulated by the defendant to commit the tort," that location would also be outside of the forum, because the "computer . . . manipulated . . . to commit the tort" was Plaintiff's phone, not Apple's servers. *See id.* As alleged in Plaintiff's Complaint, the messages transmitted from Defendants to Plaintiffs "contain[ed] an exploit and malware" before they reached Apple's servers in the United States. ECF 1 at ¶ 88. Further, as alleged in Plaintiff's Complaint, the exploit is only activated on the target's phone and only after the phone, and not the server, "receives and processes the attacker's iMessage." *Id.* at ¶ 98. Indeed, Plaintiff does not appear to allege that Defendants manipulate, transform, or otherwise commit any illegal act directly to Apple's servers, even if the attackers "interact[] with Apple's U.S.-based servers several times" in the process of sending an exploit and associated malware. *Id.* at ¶¶ 89–93. As such, this Court finds that the tortious conduct itself took place outside of the forum.

In support of her argument that purposeful availment, rather than purposeful direction, applies to the present case, Plaintiff relies heavily on an unpublished 2020 case from this district in which the court found that it could exert personal jurisdiction over foreign defendants who accessed trade secrets from a server in Oregon, even though those defendants were not physically present in Oregon when the tort was committed, because the tortious misappropriation of trade secrets occurred "at least in part . . . in Oregon." *See Climax Portable Machine Tools, Inc. v. Trawema GmbH*, No. 3:18-cv-1825-AC, 2020 WL 1304487 (D. Or. Mar. 19, 2020). *Climax* is distinguishable from the present case. In *Climax*, the plaintiffs alleged that the defendants obtained secret information stored on an Oregon server for an unauthorized purpose with an improper intent to take that information for a competing entity. *Id.* at *4. In *Climax*, in other words, the defendants did not begin the process of misappropriating the trade secrets until they reached out to the servers in Oregon, where they knew the information was stored. *Id.* at *5. In the present case, by contrast, Defendants began their tort of knowingly transmitting malware in a foreign country, because the message sent to Plaintiff's phone already contained an exploit and malware before it reached Apple's U.S.-based servers. *See* ECF 1 at ¶ 88.

Will Co. Ltd. v. Lee, a Ninth Circuit case from August of 2022 that considered personal jurisdiction over foreign defendants who access U.S.-based servers, supports this conclusion. 47 F.4th 917, 919 (9th Cir. 2022). In *Will Co. Ltd.*, the Ninth Circuit applied the purposeful direction test to analyze whether it could properly exercise jurisdiction over the defendants who ran a website that "unlawfully displayed copyrighted videos." *Id.* Notably, the servers that the defendants used to host the copyrighted conduct were located in the United States. *Id.* at 920. Nonetheless, the Court held that "in the context of tort claims . . . a defendant has the requisite minimum contacts with the forum if . . . the defendant 'purposefully direct[s]' its activities at the

forum . . . ." *Id.* at 922. In sum, given the Ninth Circuit's recent application of the purposeful direction test to a case where foreign defendants used U.S.-based servers to commit tortious acts, this Court finds that the purposeful direction test provides the proper framework for analyzing Defendants' jurisdictional challenge.

When considering whether the exercise of jurisdiction is proper under the purposeful direction test, courts within the Ninth Circuit engage in a three-step inquiry: "the defendant allegedly [must] have (1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the forum state." *Schwarzenegger*, 374 F.3d at 803 (quoting *Dole Food Co. v. Watts*, 303 F.3d 1104, 1111 (9th Cir. 2002)). Neither party disputes that Defendants committed an intentional act, but the parties do dispute whether that intentional act was expressly aimed at the United States and caused harm that Defendants knew was likely to be suffered in the United States. This Court considers each in turn.

b. Defendants' Use of Apple's U.S.-Based Servers Does Not Constitute Express Aiming at the United States

Plaintiff argues that Defendants "intentionally aimed their exploit and malware at Apple's U.S. servers to leverage vulnerabilities in Apple's iMessage system and reach [Plaintiff's] iPhone." ECF 35 at 15. In other words, Plaintiff argues that Defendants' contacts with the United States were not "fortuitous" because they intended to use Apple's U.S.-based servers to hack Plaintiff's phone. But Plaintiff's argument would force this Court to stretch the Ninth Circuit's personal jurisdiction caselaw to cover conduct that has never been found sufficient to confer jurisdiction over a foreign-based defendant.

The Ninth Circuit "has never decided that personal jurisdiction is proper over a private foreign entity solely because that entity engaged in tortious conduct from a location outside of

the United States by remotely accessing servers located in the United States." *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349, 351 (9th Cir. 2021). The defendants in *Hungerstation* were foreign corporations who allegedly accessed remote servers located in the United States and owned by third parties, and copied and transferred confidential source code and proprietary business information to servers leased by the defendants. *Id.* In affirming the district court's dismissal based on lack of personal jurisdiction, the Ninth Circuit found that "the location of the servers was fortuitous" such that the defendants' conduct could not be said to have been expressly aimed at the United States. *Id.*

Here, too, this Court finds that the location of Apple's servers in the United States is "fortuitous" such that Defendants' conduct was not expressly aimed at the United States. Plaintiff alleges that Defendants specifically targeted Apple's servers to exploit vulnerabilities in Apple's iMessage system. Accepting that allegation as true, it still does not create the type of contact between the United States and Defendants' conduct that could give rise to personal jurisdiction. Rather than showing that Defendants purposefully directed their conduct at the forum, Plaintiff's allegation, at most, shows that Defendants purposefully directed their conduct at a third party—Apple, whose choice to host their servers in the United States is entirely unrelated to the conduct at issue in Plaintiff's complaint. *Compare WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 671 (N.D. Cal. 2020) (finding an out-of-forum defendants' use of an in-forum server was "fortuitous" where "[n]either party controlled where the third parties placed their servers and the servers were not the ultimate target of the intentional act . . . .") *with Will Co., Ltd. v. Lee*, 47 F.4th 917, 924 (9th Cir. 2022) (finding an out-of-forum defendants' use of an in-forum server was not fortuitous where "*Defendants chose* to host the website in Utah . . . .") (emphasis added)); *DEX Sys., Inc. v. Deutsche Post AG*, 727 Fed. Appx. 276, 278

(9th Cir. 2018) (finding an out-of-forum defendants' use of in-forum servers was not "fortuitous" where the location of the servers was "pursuant to an agreement reached by the parties.").

Recent Ninth Circuit case law, though unpublished, supports this Court's finding that a defendant does not target a forum merely because it chooses to target a third party who in turn has chosen to do business in that forum. In *42 Ventures, LLC v. Mav*, the Ninth Circuit remanded with leave to amend a district court decision finding no personal jurisdiction where the plaintiff alleged that the defendants used U.S.-based web server companies to host purportedly infringing content. No. 20-17305, 2021 WL 5985018, at *1 (9th Cir. Dec. 16, 2021). The Ninth Circuit noted that while the allegations as pled did not show that the defendants either committed the alleged infringement in the United States or purposefully directed their infringement towards the United States, the plaintiff could potentially show purposeful direction to the United States if they could show that the defendants "deliberately choos[e] servers in the United States to enable faster service to U.S.-based customers." *Id.* Notably, the Ninth Circuit focused on the defendants' purposeful choice of the United States to reach United States customers, placing the focus of the jurisdictional inquiry squarely on the connection to the forum rather than a third party. *Id*; *see also H.B. Prods., Inc.*, 603 F. Supp. 3d at 932 (finding jurisdiction over a foreign defendant where the plaintiff's allegations "indicate[d] that Defendant sought a *United States*-based IP address to circumvent blacklist restrictions, desired a server location that would better serve his *United States* users, and profited from non-geolocated advertisements tailored to the *United States* market.") In the present case, by contrast, Plaintiff has shown only that Defendants sought to target a U.S.-based company, not the United States itself.[4]

[4] The Ninth Circuit also noted that the plaintiff in *42 Ventures, LLC* could potentially show purposeful availment by showing that the defendants "us[ed] servers in the United States to store and disseminate infringing content." No. 20-17305, 2021 WL 5985018, at *1 (9th Cir. Dec.

A survey of cases throughout the Ninth Circuit likewise supports this Court's conclusion that the choice by a third party to operate its servers in the forum is insufficient to show that a foreign defendant who uses those servers purposefully directs their actions at the forum. *See, e.g.*, *Republic of Kazakhstan v. Ketebaev*, No. 17-CV-00246-LHK, 2017 WL 6539897, at *7 (N.D. Cal. Dec. 21, 2017) (finding no personal jurisdiction because "[t]he mere fact that Google—the company that owns the servers—is headquartered in California is not enough to establish that Khrapunov, a Kazakh citizen who resides in Switzerland, expressly aimed his alleged conduct at California."); *Rosen v. Terapeak, Inc.*, No. CV-15-00112-MWF (Ex), 2015 WL 12724071, at *9 (C.D. Cal. Apr. 28, 2015) (finding no personal jurisdiction and rejecting "the notion that the mere location of a server may give rise to personal jurisdiction."); *Man-D-Tec, Inc. v. Nylube Products Co.*, LLC, No. CV-11-1573-PHX-GMS, 2012 WL 1831521, at *2 (D. Ariz. May 18, 2012) (finding no personal jurisdiction and concluding that "[i]f the mere location of a server could create personal jurisdiction, any state where a server is located would have personal jurisdiction over any user of that server."). By contrast, cases where a court has found purposeful direction often involve either tortious conduct committed in the forum state or servers owned by the plaintiff or defendant, rather than a third party. *See e.g.*, *Climax*, 2020 WL 1304487 at *4 (finding personal jurisdiction where theft of trade secrets occurred from servers located in Oregon), *DEX Sys., Inc.*, 727 F. App'x at 278 (finding purposeful direction where "the allegedly infringing *use* of [Plaintiff's] software occurred in California on [Plaintiff's] servers in

---

16, 2021). This finding supports this Court's finding that purposeful direction, rather than purposeful availment, is the proper analysis for this case. As discussed above, this case is distinct from an infringement action, where the tortious conduct does not begin until the defendant obtains and disseminates the allegedly infringing content. In the present case, the message sent by Defendants included the exploit and malware before it reached the U.S.-based servers, and the exploit and malware did not activate and infect Plaintiff's phone until it reached her in the foreign location.

Camarillo, California") (emphasis added)); *WhatsApp Inc*, 472 F. Supp. at 672 (finding purposeful direction where "defendants sought out and accessed *plaintiffs' servers* . . . ") (emphasis added)).

Mere knowledge of the location of a third-party's servers, in sum, is not sufficient to constitute purposeful direction. "Due process requires that a defendant be haled into court in a forum State based on his own affiliation with the State, not based on the 'random, fortuitous, or attenuated' contacts he makes by interacting with other persons affiliated with the State." *Walden*, 571 U.S. at 286 (citation omitted). Plaintiff's argument would ask this Court to find personal jurisdiction based on the choice of a third party not before this Court. Such an outcome is foreclosed by existing precedent and this Court declines to find the purposeful direction prong satisfied here.

c. Defendants Did Not Know That the Harm to Plaintiff Was Likely to be Suffered in the United States

The third element of the purposeful direction test requires a defendant to "caus[e] harm that the defendant knows is likely to be suffered in the forum state." *Schwarzenegger*, 374 F.3d at 803 (quoting *Dole Food Co. v. Watts*, 303 F.3d 1104, 1111 (9th Cir. 2002)). Within the Ninth Circuit, while "'the brunt' of the harm need not be suffered in the forum state," a plaintiff must nonetheless show that a "jurisdictionally sufficient amount of harm [was] suffered in the forum state." *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1207 (9th Cir. 2006) (en banc). "A defendant causes harm in a particular forum when the 'bad acts' that form the basis of the plaintiff's complaint occur in that forum." *Will Co.*, 47 F.4th at 926 (citation omitted).

This Court finds that, while the allegations in Plaintiff's Complaint support the inference that Defendants caused Plaintiff harm outside of the United States, the Complaint does not

support the inference that Defendants knew that harm was likely to be suffered in the United State as opposed to some other forum. Plaintiff argues that "[b]y uploading malicious code to Apple's U.S. servers for delivery to [Plaintiff's] iPhone, Defendants broke the digital security that is critical to [Plaintiff's] human rights work and transformed Apple's secure messaging system into Defendants' personal malware delivery device." ECF 35 at 16. But the harm to Plaintiff's device—the hack itself, and the subsequent surveillance of that device—occurred outside of the forum state. As such, the only harm that Plaintiff alleges actually occurred in the United States is the "transform[ation of] Apple's secure messaging system into . . . [a] malware delivery device." *Id.*

Plaintiff cites to no authority to support her theory that harm to a third party in the forum, rather than harm to the plaintiff, constitutes a "jurisdictionally sufficient amount of harm." *Yahoo! Inc.*, 433 F.3d at 1207. Instead, recent caselaw within the Ninth Circuit makes clear that the focus for this element of the jurisdictional analysis must be on the foreseeability of harm caused in the forum to the plaintiff, not to a third party not otherwise involved in the litigation. In *Burri Law PA v. Skurla*, for instance, the Ninth Circuit found that Arizona could exercise personal jurisdiction over three non-Arizona residents for making defamatory statements about the plaintiff, a Florida resident, when those defendants knew that the plaintiff was likely to suffer those harms in Arizona. 35 F.4th 1207, 1216 (9th Cir. 2022); *see also Dole Food Co.*, 303 F.3d at 1113 (examining whether plaintiff, "rather than its European subsidiaries," suffered harm in the forum). Based on this precedent, this Court concludes that showing harm to a third party in the forum—rather than harm to Plaintiff herself—is insufficient to satisfy the third element of the purposeful direction test.

2. Plaintiff's Claims Do Not Arise Out of Or Relate to Defendants' Forum-Related Activities

In addition to showing that the defendant purposefully directed his activities at the forum, a plaintiff must show that the claim "arise[s] out of or relate[s] to the defendant's contacts" with the forum such that "there [is] an affiliation between the forum and the underlying controversy." *Ford Motor Co.*, 141 S. Ct. at 1025 (citations omitted). While this standard does not require the plaintiff to show that the defendant's actions were the but-for cause of the plaintiff's claim, "the phrase 'relate to' incorporates real limits, as it must to adequately protect defendants foreign to a forum." *Id.* at 1026. Plaintiff's argument that her claim arises out of or relates to Defendants' contacts with the forum mirrors her argument that Defendants purposefully directed their activities towards the forum: that "Defendants' contacts with U.S. servers . . . were necessary to infecting [Plaintiff's] iPhone with malware." ECF 35 at 22.

As discussed above, Plaintiff's argument fails because it requires this Court to impart the affiliation between a third party and the forum to Defendants. This type of logic is foreclosed by the Supreme Court's decision in *Walden v. Fiore*, which emphasized that the relationship between the defendant and the forum "must arise out of contacts that the 'defendant *himself*' creates with the forum State." 571 U.S. at 284. In reiterating that it had "consistently rejected attempts to satisfy the defendant focused 'minimum contacts' inquiry by demonstrating contacts between the plaintiff (or third parties) and the forum State," *id.* at 284, the Supreme Court held that a petitioner's knowledge of the respondent's "strong forum connections" was insufficient to confer personal jurisdiction over petitioner where none of the tortious conduct at issue occurred in the forum, *id.* at 288–89. Accepting Plaintiff's argument would likewise require this Court to exercise personal jurisdiction over Defendants based solely on their knowledge of the third-party's contacts with the United States.

Plaintiff alternatively argues that her claim arises out of or relates to Defendants contacts with the forum because "Defendants[']s other U.S.-based contacts—including the acquisition of exploits, reliance on U.S. technology and knowhow illegally transferred from CyberPoint, employment of U.S. individuals, and U.S. anonymization services—were essential to the operation of Project Raven and thus to the hack against [Plaintiff]." ECF 35 at 22. Defendants counter that these "other U.S.-based contacts" are unrelated to the conduct that ultimately underpins Plaintiff's claim, which is the allegedly tortious hack of Plaintiff's phone caused by malware. This Court agrees that Plaintiff has failed to plead with sufficient specificity how this background conduct relates to the use of specific malware to infect Plaintiff's phone. The technology that Defendants purchased from U.S.-based companies was altered in significant ways before being deployed in the hack of Plaintiff's phone. Additionally, the fact that Defendants may have developed expertise and knowhow in the forum that was later used to create the malware that infected Plaintiff's phone is not enough to confer jurisdiction.

3. Exercise of Jurisdiction Over DarkMatter Would be Unreasonable

If the plaintiff satisfies the first two prongs of the "minimum contacts" analysis, the burden then shifts to the defendant "to set forth a 'compelling case' that the exercise of jurisdiction would not be reasonable." *CollegeSource*, 653 F.3d at 1076. To evaluate reasonableness, courts within the Ninth Circuit use a seven-factor balancing test that weighs:

> (1) the extent of the defendant's purposeful interjection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

Freestream, 905 F.3d at 607 (citation omitted).

As noted above, this Court finds that Plaintiff has failed to meet either the first or second prong of the "minimum contacts" analysis. Even if Plaintiff had shown that Defendants had sufficient "minimum contacts" with the United States, however, this Court would still find that the exercise of jurisdiction over Defendants would be unreasonable.

First, this Court finds that Defendants' allegedly tortious conduct—sending an iMessage from a foreign location, transmitted through U.S.-based servers, to a foreign phone with intent to hack the phone in the foreign locale—presents no "purposeful interjection" into United States' affairs, for the reasons discussed above with respect to the "purposeful direction" analysis. *See Paccar Int'l, Inc. v. Com. Bank of Kuwait, S.A.K.*, 757 F.2d 1058, 1065 (9th Cir. 1985) (finding "negligible" purposeful interjection where defendants actions in the forum were "aimed at a nonresident"). As such, the Court finds that this factor weighs in favor of finding that jurisdiction would be unreasonable.

Second, this Court finds that Defendants would face at least some burden if they were forced to defend the action in the United States. *See id.* (finding that the burden placed on a defendant, based in Kuwait, in defending a suit in California, "support[ed] a finding that exercising jurisdiction [was] unreasonable"); *accord Asahi Metal Indus. Co. v. Superior Court*, 480 U.S. 102, 114 (1987) ("The unique burdens placed upon one who must defend oneself in a foreign legal system should have significant weight in assessing the reasonableness of stretching the long arm of personal jurisdiction over national borders."). There are, however, several factors that mitigate this burden, at least with respect to Defendants Baier, Gericke, and Adams. All three are U.S. citizens who speak, read, and write English. *See Dole Food Co.*, 303 F.3d at 1115 (finding that the burden on foreign defendants was lessened where the defendants were fluent in English, received degrees from U.S. universities, and had traveled to the United States

previously). Plaintiff further argues that all Defendants, including Defendant DarkMatter, are involved in other legal proceedings in the United States. ECF 35 at 23. As such, the second factor cuts against Defendants and in favor of Plaintiff.

As to the third factor—the extent of conflict with the sovereignty of the defendant's state—this Court finds that this factor weighs in favor of finding that jurisdiction would be unreasonable. Although Plaintiff attempts to cast the implications of this suit narrowly, by arguing that it concerns only the determination of U.S. laws against the individual and private corporations involved, Plaintiff also admits that her claims "relate to conduct carried out at the behest of the UAE government." ECF 35 at 24. This Court must consider both the "procedural and substantive interests of other nations" in deciding whether to exercise jurisdiction. *Asahi Metal Indus. Co.*, 480 U.S. at 115. In this instance, the fact that Plaintiff's conduct relates to actions carried out at the direct behest of a foreign sovereign counsels against exercising jurisdiction.

This Court likewise finds that the fourth factor—the forum's interest in adjudicating the dispute—weighs against the exercise of jurisdiction. While the United States has a strong interest in providing a forum for its residents who are injured by tortious conduct, Plaintiff is not a United States resident. The United States might have a strong interest in ensuring that its U.S.-based companies who rely on U.S.-based servers are not subject to transmissions of malware, but Apple is not a party to this action and its interests cannot be considered in determining whether jurisdiction is reasonable. The Ninth Circuit has warned against expanding jurisdiction under Rule 4(k)(2) in situations where the foreign defendants have had only limited contacts with the United States. *See Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.*, 284 F.3d 1114, 1123, 1126–27 (9th Cir.2002) (quoting *Burger King Corp.*, 471 U.S. at 475) (holding that

a defendant should not be haled into court as a result of "random," "fortuitous," or "attenuated" contacts and declining to exercise Rule 4(k)(2) jurisdiction when the foreign defendant made fifteen individual shipments to California and seven individual shipments to the East Coast over the course of thirteen years).

As to the fifth factor, this Court finds that the United States would not offer the most efficient judicial resolution for the controversy. Plaintiff argues that "Apple's technology experts and the companies that designed and sold the exploits used by Defendants" are located in the United States, but also admits that "'relevant parties, documents, and witnesses'" are located abroad. ECF 35 at 25. Though the Ninth Circuit has opined that the burden of adjudicating a dispute based on foreign evidence and witnesses "is no longer weighed heavily given the modern advances in communication and transportation," *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1323 (9th Cir. 1998), the almost completely foreign nature of the tortious conduct at issue weighs slightly in favor of Defendants.

This Court agrees with Plaintiff that the sixth factor—the importance of the forum to the plaintiff's interest in convenient and effective relief—weighs in favor of jurisdiction. Plaintiff brings her claims under U.S. law, which heightens Plaintiff's interest in her claims being adjudicated by a U.S. court. The seventh factor—the availability of an alternative forum—also favors Plaintiff. Plaintiff argues that "the Complaint's allegations show that the UAE is not a viable alternative forum." ECF 35 at 25. This Court agrees that Plaintiff's Complaint alleges conduct by the UAE that, if assumed to be true, would make the UAE a hostile forum to Plaintiff's claims. *See* ECF 1 at ¶¶ 32, 74, 113 (alleging that the UAE targets human rights defenders generally and targeted Plaintiff specifically using technology deployed by Defendants). The fact that the second, sixth, and seventh factors favor Plaintiff, however, is not

sufficient to overcome the conclusion that the other reasonableness factors weigh against jurisdiction.

CONCLUSION

For the foregoing reasons, this Court finds that it cannot exercise jurisdiction over Defendants consistent with due process. As such, Defendants' Motion to Dismiss is GRANTED. This Court notes, however, that there may be certain factual allegations that Plaintiff could add to her Complaint to satisfy the exercise of jurisdiction over Defendants. Plaintiff's Complaint is therefore dismissed without prejudice and with leave to amend. If Plaintiff chooses to amend, Plaintiff is ordered to notify this Court within fourteen days and file her Amended Complaint within thirty days of the issuance of this Opinion and Order.

IT IS SO ORDERED.

DATED this 16th day of March, 2023.

/s/ Karin J. Immergut
Karin J. Immergut
United States District Judge